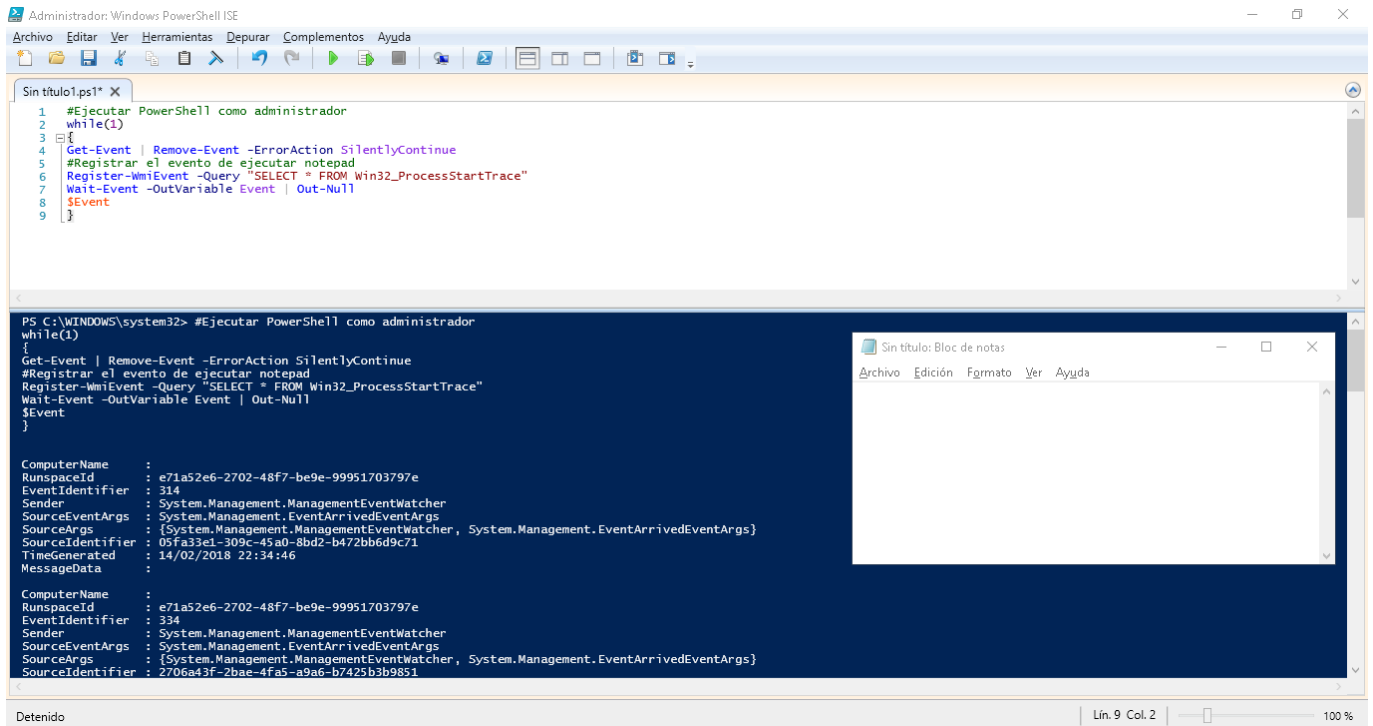


Registrar y mostrar un evento en PowerShell cuando se ejecuta un programa

[crayon-6a9d7020b23aa223633131/]



```
Sin título1.ps1 X
1 #Ejecutar PowerShell como administrador
2 while(1)
3 {
4   Get-Event | Remove-Event -ErrorAction SilentlyContinue
5   #Registrar el evento de ejecutar notepad
6   Register-WmiEvent -Query "SELECT * FROM Win32_ProcessStartTrace"
7   Wait-Event -OutVariable Event | Out-Null
8   $Event
9 }

PS C:\WINDOWS\system32> #Ejecutar PowerShell como administrador
while(1)
{
  Get-Event | Remove-Event -ErrorAction SilentlyContinue
  #Registrar el evento de ejecutar notepad
  Register-WmiEvent -Query "SELECT * FROM Win32_ProcessStartTrace"
  Wait-Event -OutVariable Event | Out-Null
  $Event
}

ComputerName      :
RunspaceId        : e71a52e6-2702-48f7-be9e-99951703797e
EventIdentifier    : 314
Sender            : System.Management.ManagementEventWatcher
SourceEventArgs   : System.Management.EventArrivedEventArgs
SourceArgs        : {System.Management.ManagementEventWatcher, System.Management.EventArrivedEventArgs}
SourceIdentifier   : 05fa33e1-309c-45a0-8bd2-b472bb6d9c71
TimeGenerated      : 14/02/2018 22:34:46
MessageData       :

ComputerName      :
RunspaceId        : e71a52e6-2702-48f7-be9e-99951703797e
EventIdentifier    : 334
Sender            : System.Management.ManagementEventWatcher
SourceEventArgs   : System.Management.EventArrivedEventArgs
SourceArgs        : {System.Management.ManagementEventWatcher, System.Management.EventArrivedEventArgs}
SourceIdentifier   : 2706a43f-2bae-4fa5-a9a6-b7425b3b9851
```

Detenido | Lin. 9 Col. 2 | 100 %